UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Gary Hall, *on behalf of himself and all others similarly situated*,

Plaintiff,

v.

Centerspace, LP, and Centerspace, Inc.,

Defendants.

No. 22-cv-2028 (KMM/DJF)

ORDER

In November of 2021, Centerspace LP learned that computer hackers accessed its data systems, including files containing the personal identifying information of the company's customers and employees. After investigating the incident, in July of 2022, Centerspace LP notified the people whose information may have been exposed, including Plaintiff Gary Hall. Mr. Hall filed a class-action Complaint, alleging that the company's improper handling of its data security caused the unauthorized exposure of his personal information to third parties. Defendants Centerspace LP and Centerspace, Inc. seek dismissal of Mr. Hall's Complaint pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). For the reasons that follow, Defendants' motion is granted in part and denied in part.

BACKGROUND

Centerspace LP and Centerspace, Inc.,[1] own and operate apartment complexes in Colorado, Minnesota, Montana, North Dakota, and South Dakota. [Compl. ¶ 26, Dkt. 2.] Mr. Hall was an employee of IRET Property Management, a Centerspace LP subsidiary or its predecessor.[2] Mr. Hall's employer was a property manager for the Centerspace-owned apartment complexes. [*Id.* ¶¶ 27, 38.]

Mr. Hall was required to provide his personal identifying information ("PII") to his employer. Similarly, other Centerspace employees, prospective employees, tenants, and prospective tenants were required to give Defendants their PII as a condition of their housing or employment relationships. The PII includes names, bank account information, and social security numbers. [*Id.* ¶ 28.] Mr. Hall trusted that Centerspace LP would use reasonable measures to protect his PII according to its internal policies and state and federal law. [*Id.* ¶ 40.]

On November 11, 2021, Centerspace LP learned that it had experienced a data security breach, which disrupted access to its computer systems. [*Id.* ¶ 32.] Centerspace looked into the incident, hiring independent digital forensics analysts and an incident response firm. [*Id.*] On Nov. 15th, the company discovered that computer files potentially

[1] The Complaint names both Centerspace LP and Centerspace, Inc. as Defendants, but refers to them collectively throughout as "Centerspace." The Complaint does not allege the relationship between the two companies.

[2] The Complaint refers to IRET as a "subsidiary" of Centerspace, but it also cites to a Centerspace Annual Report from 2021 which indicates that Centerspace LP was "formerly known as IRET Properties." [Compl. ¶ 38 n.5.]

containing PII were accessed by unauthorized third parties. [*Id.*] However, Centerspace LP did not notify those potentially affected by the data breach until July 2022. [*Id.* ¶¶ 17, 34; *id.*, Ex. A, Dkt. 2-1.] The data breach affected 8,190 people, including current and former employees and current and former tenants. [*Id.* ¶ 4.]

On information and belief, Mr. Hall alleges that Centerspace "failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over consumer PII." [*Id.* ¶ 35.] Defendants allegedly acted negligently by failing to prevent the data breach and to stop cybercriminals from accessing the PII that they maintain. [*Id.*] The Complaint asserts that Defendants were unable or unwilling notify current and former employees and tenants about the breach without unreasonable delay. [*Id.* ¶ 36.] And Defendants allegedly waited until after the data breach to implement digital security measures to make future breaches of their systems less likely. [*Id.* ¶ 37.]

Further, Mr. Hall alleges that because of the data breach he has experienced several types of harms. He has already and will continue to spend "considerable time and effort monitoring his accounts to protect himself from identity theft." [*Id.* ¶ 41.] He has concerns about his financial security and is uncertain about what information was exposed in the data breach. The breach has caused him to experience "feelings of anxiety, sleep disruption, stress, fear, and frustration." [*Id.*] Mr. Hall asserts that he and the proposed members of the class have suffered monetary losses, lost time, anxiety, and emotional distress. [*Id.* ¶ 43.] In addition, they have suffered or are at an increased risk of suffering the following harms: (a) lost opportunity to control use of their PII; (b) diminution in value of their PII;

(c) compromise and publication of their PII; (d) out-of-pocket costs associated with prevention, detection, recovery, and remediation from identity theft or fraud; (e) lost opportunity costs and lost wages associated with time and effort to address or mitigate the consequences of the Data Breach; (f) delayed receipt of tax refunds; (g) unauthorized use of stolen PII; and (h) continued risk to their PII, which remains in Defendants' possession.[3] [*Id.* ¶ 43(a)–(h).]

In explaining why Defendants are responsible for these harms, Mr. Hall alleges that Defendants failed to adhere to Federal Trade Commission ("FTC") guidelines in protecting the PII they possessed. This includes failure to follow FTC recommendations for how to safeguard their computer systems and to monitor their systems to allow for quick responses to a data breach. The FCC recommends steps such as maintaining information no longer than necessary for a transaction; limiting access to sensitive data; requiring complex passwords to be used on networks; using industry-tested methods for security; monitoring for suspicions activity on the network; and verifying that third-party service providers have implemented reasonable security measures. [*Id.* ¶ 52–57.] Mr. Hall asserts that the Defendants' failure to follow the FTC's recommendations constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. [*Id.* ¶ 56.]

[3] In addition, the Complaint explains how stolen PII can be distributed on the black market, including through so-called "Fullz packages" which are dossiers compiled to match stolen PII with unregulated publicly available data. [*Id.* ¶¶ 46–47.] The Complaint stops short of clearly alleging that a Fullz package regarding Mr. Hall has been compiled by any third party based on PII unlawfully accessed in the Centerspace data breach.

Mr. Hall seeks to represent a class of "all individuals residing in the United States whose PII was compromised in the Data Breach disclosed by Centerspace in July 2022." [*Id.* ¶ 58.] He brings the following claims: negligence (Count I); breach of implied contract (Count II); unjust enrichment (Count III); and declaratory judgment (Count IV). In his Prayer for Relief, he seeks certification of the class, declaratory and injunctive relief, damages, restitution, attorneys' fees and costs, interest, and other appropriate relief.

DISCUSSION

In their motion to dismiss, Defendants challenge Mr. Hall's standing under Article III of the Constitution to assert claims against Centerspace, Inc.[4] and to pursue future injunctive relief. Defendants also argue that Mr. Hall's remaining claims should be dismissed for failure to state a claim. The Defendants' motion is granted in part and denied in part.

I. Standing

A. Legal Standard

Defendants' arguments regarding Article III standing present a challenge to the Court's subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1). Defendants' arguments raise a "facial" challenge. *See Osborn v. United States*, 918 F.2d

[4] Plaintiff agreed that the Court could dismiss the claims against Centerspace, Inc. in response to Defendants' motion. Based on that concession, the Court grants the Defendants' motion to the extent it seeks dismissal of Centerspace, Inc, and the dismissal will be without prejudice. Because Centerspace, Inc., will no longer be a party to this action, for the remainder of this Order, the Court refers to Centerspace LP as "Centerspace."

724, 729 n.6 (8th Cir. 1990) (noting that a facial challenge to subject matter jurisdiction looks only at the pleadings and essentially applies the Rule 12(b)(6) standard). When considering a facial challenge to jurisdiction, courts presume the facts alleged in the complaint to be true. *Titus v. Sullivan*, 4 F.3d 590, 593 (8th Cir. 1993). For a plaintiff to meet his burden to allege Article III standing he must show (1) an injury in fact that (2) is fairly traceable to the defendant's alleged conduct and (3) is likely to be redressed by a favorable court ruling. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992).

Although this is a putative class action, as the named plaintiff, Mr. Hall must still allege facts establishing the elements of his own standing, and may not rely on the injuries of unidentified class members. *Spokeo*, 578 U.S. at 338 & n.6; *In re SuperValu, Inc.* ("*SuperValu I*"), 870 F.3d 763, 768 (8th Cir. 2017) (same).

B. Count IV - Declaratory and Injunctive Relief

In Count IV of the Complaint, Mr. Hall seeks a judgment declaring that Centerspace "owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII with which it is entrusted, and to notify impacted individuals of the data Breach under the common law and Section 5 of the FTC Act." [Compl. ¶ 96(a).] The declaratory judgment he seeks would also include a declaration that Centerspace breached, "and continues to breach, its duty by failing to employ reasonable measures to secure" the relevant PII, and that such breach "continues to cause harm to Plaintiff and the Class." [*Id.* ¶¶ 96(b)–(c).] In addition to seeking that declaratory relief, Mr. Hall asserts that the Court "should also issue corresponding injunctive relief requiring Defendants to employ adequate

security protocols consistent with industry standards to protect its clients' (i.e. Plaintiff's and the Class's) data." [Compl. ¶ 97; *see also id.* ¶¶ 98–100 & Prayer for Relief ¶ C.]

Centerspace argues that Mr. Hall lacks standing to pursue declaratory or injunctive relief. Centerspace contends that there are no facts in the pleading indicating that there is a substantial risk of future harm that would be redressed by the requested declarations or injunction. Centerspace states that "just because there was one cyberattack against Centerspace[], there is no support for the notion that another one is imminent or that a future data security incident would lead to misuse of this Plaintiff's data." [Defs.' Mem. at 4, 9–10.] In response, Mr. Hall notes that he has alleged that Centerspace continues to store employee and tenant PII without adequate data security measures in place to protect it from unauthorized third-party access, and he argues that this is sufficient to demonstrate that an injury is clearly impending or that there is a substantial risk that harm will occur. [Pl.'s Resp. at 4–5.]

Because "a plaintiff must demonstrate standing separately for each form of relief sought," courts in data breach cases have considered whether plaintiffs have standing to seek injunctive and declaratory relief. *In re Pawn Am. Consumer Data Breach Litig.* ("*Pawn Am.*"), Case No. 21-CV-2554 (PJS/JFD, 2022 WL 3159874, at *3 (D. Minn. Aug. 8, 2022) (quoting *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210 (2021)) (cleaned up). As the *Pawn America* court observed, the "risk of real harm" can suffice as a concrete injury for purposes of standing. *Id.* at *2 (quoting *Spokeo*, 578 U.S. at 341) (*Pawn Am.*'s emphasis removed). "In future injury cases, the plaintiff must demonstrate that the

threatened injury is certainly impending or there is a substantial risk that the harm will occur." *SuperValu I*, 870 F.3d at 769.

Similar to the request in Mr. Hall's Complaint, in *Pawn America* the plaintiffs sought "forward-looking" relief in the form of a declaratory judgment and injunction that would force the defendant "to implement various data-security measures to ensure that, going forward, [defendant] 'adequately safeguards' plaintiffs' data." 2022 WL 3159874 at *3. The court found that the plaintiffs lacked standing to pursue these forms of relief because they failed to "allege a 'sufficiently imminent and substantial' risk of harm that would be avoided if the sought-after relief was granted." *Id.* (quoting *TransUnion*, 141 S. Ct. at 2210). The court explained that the injunction and declaration requested by the *Pawn America* plaintiffs would only address harm caused by a future breach of the defendant's data systems. *Id.* Although it was possible a second breach could occur, which could in turn harm the plaintiffs, the court found this insufficient to confer standing with respect to the forward-looking declaration and injunction because "the law requires not just possibility but *imminence*." *Id.* (emphasis in original).

The same is largely true here. A declaration that Centerspace continues to owe a legal duty to Mr. Hall and the class, continues to breach that duty, and continues to cause Mr. Hall and the class harm is aimed at an injury that would be caused by a future attack of the Defendant's network. The same is true of entering an injunction requiring Centerspace to employ adequate security protocols to protect Mr. Hall's and the Class's PII—the injunction would be aimed at decreasing the likelihood of a future data breach that could expose the sensitive data. For Mr. Hall to have standing to pursue this relief, he

is required to show that he faces a sufficiently imminent and substantial risk of future harm that they address. *Pawn Am.*, 2022 WL 3159874, at *3. The Complaint falls short of this requirement. For instance, there are no facts in the Complaint that indicate a second data breach is certainly impending, or even that there is a substantial risk one will occur. There is, for example, no suggestion that Centerspace is currently being targeted by hackers, or that something about their operations makes them uniquely vulnerable to incursions. Nothing in Mr. Hall's pleading transforms the *possibility* that Centerspace might suffer another data breach into an imminent or substantial risk.[5]

Mr. Hall's arguments to the contrary fail to persuade the Court that the allegations in this Complaint describe the imminence required. First, Mr. Hall argues that *Pawn America* is "simply inapplicable" because the parties did not brief the issue of standing in that case and the court raised it on its own. [Pl.'s Resp. at 6 n.2.] Even if that is true, a federal court's *sua sponte* consideration of its subject matter jurisdiction does not make the court's analysis any less valuable in illustrating the proper application of a legal rule. And Mr. Hall fails to explain how Judge Schiltz's decision might have diffred if aided by additional briefing. The posture in which the jurisdictional issue arose does not undermine the *Pawn America* court's reasoning.

[5] Aside from the components of the requested declaratory judgment that are forward looking, the Declaratory Judgment claim in Count IV of the Complaint can also be read to seek a declaration of the parties' rights and legal relations retrospectively. Because the parties' briefing does not address any aspect of Count IV other than the forward-looking aspects of the declaratory and injunctive relief requested, the Court does not dismiss any request for retrospective declaratory relief.

Second, the Court disagrees that *In re: Netgain Technology, LLC* ("*Netgain*"), No. 21-cv-1210 (SRN/LIB), 2022 WL 1810606 (D. Minn. June 2, 2022), requires a contrary result on this issue. Mr. Hall relies on a portion of the *Netgain* opinion addressing whether the plaintiffs had stated a claim for declaratory and injunctive relief pursuant to Fed. R. Civ. P. 12(b)(6), not the *Netgain* court's discussion of standing. *Id.* at *17 (finding the defendant's arguments concerning the merits to be premature). But the threshold inquiry of standing and the allegations needed to clear the hurdles of Rule 8(a) and 12(b)(6) are distinct, *See SuperValu I*, 870 F.3d at 773, so the language in *Netgain* Mr. Hall relies upon is less persuasive. Moreover, although the *Netgain* court did not dismiss on the basis of standing, the court's discussion of future harm did not specifically address whether the *Netgain* plaintiffs had standing to obtain forward-looking declaratory and injunctive relief that would redress harm from a possible future data breach. *Id.* at *5. The *Netgain* court's discussion of standing simply does not address the specific issue presented here.

It should be clear from this discussion that the Court is not suggesting that forward-looking injunctive relief is never appropriate in a data breach case. Indeed, in *Perry v. Bay & Bay Transportation Services, Inc.*, Civil No. 22-973 (JRT/ECW), --- F. Supp. 3d ---, 2023 WL 171885 (D. Minn. Jan. 12, 2023), decided after the briefing was complete in this matter, another judge in this district found the allegations in a complaint sufficient to sustain a request for forward-looking injunctive and declaratory relief. It is unclear whether *Perry*'s reasoning in finding standing to pursue such relief is entirely consistent with *Pawn America*'s, but the allegations concerning the misuse of the plaintiff's PII in *Perry* are far more substantial than any allegations in Mr. Hall's Complaint. 2023 WL 171885, at *3–4

(plaintiff alleged his PII was published on the dark web and that he was the victim of a bank scam "where cyberthieves used his PI disclosed in [defendant's] data breach to contact him and impersonate his bank and scam him out of $500").

For these reasons, the Court finds that Mr. Hall has not demonstrated standing for his forward-looking claims for a declaratory judgment and injunctive relief and those aspects of Count IV must be dismissed without prejudice for lack of jurisdiction. Centerspace has not otherwise challenged Mr. Hall's standing, and the Court has found no other inadequately pled issue of standing.

II. Failure to State a Claim

A. Legal Standard

Defendants argue that Mr. Hall's claims for breach of implied contract, unjust enrichment, and negligence should be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). Applying Rule 12(b)(6), a court must accept as true the factual allegations in the complaint and draw all the reasonable inferences in the plaintiff's favor. *Gorog v. Best Buy Co.*, 760 F.3d 787, 792 (8th Cir. 2014). Detailed allegations are not required, but they must be enough to "raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). The complaint must "state a claim to relief that is plausible on its face." *Id.* at 570. A claim is plausible when the facts allow the court to draw the reasonable inference that the defendant is liable for engaging in the alleged conduct. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

B. Count II - Breach of Implied Contract

To state a claim for breach of contract under Minnesota law,[6] a plaintiff must allege facts showing that (1) a contract was formed, (2) the plaintiff performed any conditions precedent, (3) the defendant materially breached the contract, and (4) damages. *Gen. Mills Operations, LLC v. Five Star Custom Foods, Ltd.*, 703 F.3d 1104, 1107 (8th Cir. 2013). "Under the common law of Minnesota, contracts of any sort can be implied in fact and can be oral or written." *Perry v. Bay & Bay Transp. Servs., Inc.*, Civil No. 22-973 (JRT/ECW), --- F. Supp. 3d ---, 2023 WL 171885, at *9 (D. Minn. Jan. 12, 2023) (citing *McArdle v. Williams*, 258 N.W. 818, 820–21 (Minn. 1935). Courts evaluate whether an implied contract was formed by considering the "objective manifestations of the parties' words, conduct, and documents, and not by their subjective intent." *Id.* (quoting *Holman Erection Co. v. Orville E. Madsen & Sons*, 330 N.W.2d 693, 695 (Minn. 1983)).

Centerspace argues that Mr. Hall's Complaint fails to allege either a meeting of the minds concerning the security of his PII or a breach by Centerspace. [Def.'s Mem. at 11–13.] The Court finds that the Complaint plausibly alleges a breach-of-implied-contract claim. Mr. Hall asserts that he was an employee of IRET, a Centerspace subsidiary or predecessor, and to obtain and maintain employment, Centerspace required Mr. Hall to provide his PII to the company. Centerspace also allegedly implicitly "agreed it would safeguard the data according to its internal policies and state and federal law." [Compl.

[6] As this is a diversity action, the parties agree that for purposes of the motion to dismiss the Court should apply the substantive law of Minnesota.

¶ 30; *see also id.* ¶¶ 74–75 (stating that the agreement not to disclose and safeguard the data was implicit).] Mr. Hall therefore has alleged facts indicating that he offered to provide the PII in exchange for Centerspace's offer of employment and its implicit offer of data safeguarding.

Relying on *Longenecker-Wells v. Benecard Services*, 658 F. App'x 659, 662 (3d Cir. 2016), Centerspace argues that these allegations do not suffice because the promises at issue are not for data protection, but for employment (in Mr. Hall's case), and for housing in exchange for rent (in the case of the absent tenant class members). However, *Longenecker-Wells* is of limited usefulness here because it does not apply Minnesota law. Other courts considering Minnesota law have found allegations similar to those in Mr. Hall's Complaint sufficient to show formation of an implied contract. *See Perry*, 2023 WL 171885, at *9. Moreover, the Court agrees with courts that have declined to rely on *Longenecker-Wells*'s reasoning because the facts alleged in complaints like Mr. Hall's permit the reasonable inference that requiring someone to provide a Social Security number and other sensitive personal information as part of a transaction carries with it the recipient's implied agreement to reasonably safeguard it. *Mackey v. Belden, Inc.*, Case No. 4:21-CV-00149-JAR, 2021 WL 3363174, at *9 (E.D. Mo. Aug. 3, 2021).

Centerspace also relies on *Kuhns v. Scottrade, Inc.*, 868 F.3d 711 (8th Cir. 2017), to argue that Mr. Hall failed to adequately allege a breach, but the Court finds that *Kuhns* does not require dismissal of the implied-contract claim here. For one thing, *Kuhns* does not apply Minnesota law. But more importantly, Centerspace attempts to compare the inadequacy of the plaintiffs' showing in *Kuhns* to this case based on a narrow and

procedurally improper reading of the Complaint. Centerspace's brief implies that the only facts relevant to considering the implied-contract claim are found in the seven paragraphs that comprise Count II. [Defs.' Mem. at (citing only Compl. ¶¶ 74–80).] But it is widely understood that when considering a Rule 12(b)(6) motion, a court reads the complaint as a whole. *Braden v. Wal-Mart Stores, Inc.*, 588 F.3d 585, 594 (8th Cir. 2009) ("[T]he complaint should be read as a whole, not parsed piece by piece to determine whether each allegation, in isolation, is plausible."). Elsewhere in the Complaint, Mr. Hall specifically asserts how Centerspace failed to comply with industry standards, failed to adequately train its employees on reasonable cybersecurity practices, failed to follow several FTC guidelines like those applicable to encryption of data, and delayed providing prompt notice upon discovery of the data breach, all of which allegedly contravene the implicit promise it made to act reasonably in safeguarding his data. These are sufficient facts to plausibly allege a breach.

Finally, Centerspace argues that Mr. Hall fails to state an implied-contract claim because his assertions of harm are too speculative in the absence of allegations that any person actually experienced an incident of fraud or identity theft. [Def.'s Mem. at 13.] Again the Court disagrees, but because the arguments completely overlap, the Court will discuss the issue in the context of the negligence claim below. *See In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014) (explaining that the defendant's argument that plaintiffs failed to establish any damages flowing form an alleged breach of implied contract "merely restate[d]" its argument that they hadn't alleged any damages at all, which the court found to be "incorrect").

C. Count III - Unjust Enrichment

To state a claim for unjust enrichment, a plaintiff must allege facts showing that the plaintiff conferred a benefit on the defendant, the defendant appreciated and knowingly accepted the benefit, and the defendant's acceptance and retention of the benefit under the circumstances would be unjust or inequitable. *Dahl v. R.J. Reynolds Tobacco Co.*, 742 N.W.2d 186, 195 (Minn. Ct. App. 2007); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1177 (citing *ServiceMaster of St. Cloud v. GAB Bus. Servs., Inc.*, 544 N.W.2d 302, 306 (Minn. 1996)).

Centerspace argues that Mr. Hall's unjust enrichment claim fails because he does not allege a benefit was conferred on Centerspace.[7] Centerspace contends that neither the personal information Mr. Hall gave to the company, nor the employment services he provided, can serve as the benefit conferred for purposes of this claim. Further, Centerspace asserts no portion of any tenant's rent or the value of any PII that was given to Centerspace was allegedly provided for the purpose of securing data protection, undermining any claim of unjust enrichment per the reasoning of *Carlsen v. GameStop, Inc.*, 833 F.3d 903 (8th Cir. 2016). In response, Plaintiff argues that he has adequately alleged an unjust enrichment claim because he asserts that Centerspace required he provide it with his PII, and then

[7] In its brief, Centerspace quotes the allegation from paragraph 38 of the Complaint that states IRET is "subsidiary of Centerspace." [Defs.' Mem. at 14.] To the extent Centerspace suggests that the flaw with Mr. Hall's unjust enrichment claim is that any benefit would have been conferred on an entity that is legally distinct from Centerspace because it is a "subsidiary," the Court is not persuaded that the claim fails for this reason. The Complaint also indicates that IRET Property Management is simply the business entity that is the predecessor to Centerspace LP. [Compl. ¶ 38 n.5.]

Centerspace retained the benefit of the PII and the benefit of his employment services. [Pl.'s Mem. at 10.]

The Court concludes that Mr. Hall has not adequately alleged an unjust enrichment claim. He does not identify a benefit plausibly conferred upon Centerspace through the provision of PII. The Court agrees that *Carlsen* is instructive. In *Carlsen*, the named plaintiff subscribed to an online magazine, which he accessed through a website, and for which he paid an annual subscription fee to the defendant GameStop. 833 F.3d at 907. Carlsen shared his PII with GameStop, and through its privacy policy, GameStop agreed not to share his PII with anyone. But Carlsen alleged that GameStop embedded Facebook source code on the website that resulted in unauthorized exposure of his PII to others, and if he had known that his information would be disclosed in this way, he would not have paid for the subscription or accessed the magazine's online content. *Id.* Carlsen claimed unjust enrichment, asserting "that the benefit conferred on GameStop 'is the money that GameStop took from him in exchange for the Privacy Policy that it chose to ignore.'" *Id.* at 912 (brackets removed). Applying Minnesota law, the *Carlsen* court concluded that the unjust-enrichment claim failed as a matter of law because Carlsen did not "allege that any specific portion of his subscriber fee went toward data protection or that GameStop agreed to provide additional protection to paid subscribers that it did not also provide to non-paid subscribers." *Id.* Consequently, the court found that Carlsen had not conferred a benefit on GameStop in exchange for protection of his PII. *Id.*

The *Carlsen* case is not the only authority which undermines Mr. Hall's unjust enrichment claim. In data-breach litigation involving Target Corporation discussed above,

the court found the plaintiffs failed, in part, to state an unjust enrichment claim based on similar reasoning. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1177–78. There, the plaintiffs suggested that Target sold its goods at a premium, essentially agreeing to provide adequate data security for consumers' PII in exchange for the markup on its goods. *Id.* The court found no merit to this theory:

> Target charges all shoppers the same price for the goods they buy whether the customer pays with a credit card, debit card, or cash. But cash customers face no risk that a computer hacker will steal their personal financial information. If Target charged credit- and debit-card customers more for their purchases to offset the costs of data security, Plaintiffs might have a plausible allegation in this regard. But the fact that all customers regardless of payment method pay the same price renders Plaintiffs' overcharge theory implausible.

Id.

This same reasoning undermines Mr. Hall's unjust enrichment claim here. Mr. Hall posits that he conferred a benefit on Centerspace in the form of his employment services and the value of his PII, and Centerspace unjustly retained that benefit without providing adequate data security. But like the exchange of a subscription fee for access to an online magazine in *Carlsen*, the plausibly alleged exchange here is Mr. Hall's employment services for the wages he was paid by Centerspace while he worked there. Nothing in the Complaint suggests that Mr. Hall or any other employee provided more or more valuable employment services in exchange for greater data protection. The same is also true of the allegations concerning the purported class of current and former Centerspace tenants—the relevant exchange is housing for rent, but there are no allegations that tenants who provided

Centerspace their PII paid more in rent to secure greater data security than those who did not provide their PII. Consequently, the Court concludes that Mr. Hall fails to state a plausible unjust enrichment claim.[8]

D. Negligence

Finally, Centerspace asks the Court to dismiss Plaintiff's negligence claim. To state a claim for negligence under Minnesota law, Mr. Hall must allege a duty, breach, causation, and damages. *Netgain*, 2022 WL 1810606, at *8 (citing *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1170). Here, Centerspace argues that Mr. Hall has failed to allege a plausible negligence claim because his claims of future harm are too speculative. [Defs.' Mem. at 15–17.] As noted above, Centerspace makes the same argument with respect to Mr. Hall's implied-contract claim. [*Id.* at 13.]

Plaintiff's Complaint adequately alleges damages sufficient to support claims for negligence and breach of an implied contract. Mr. Hall has alleged that the exposure of his PII has placed him at risk of identity theft now and in the future. He also asserts that the value of his PII has been diminished and that he has had to spend time monitoring his accounts to protect himself from identity theft and fraud. [Compl. ¶¶ 41–43.] Moreover, as

[8] Mr. Hall cites several out-of-circuit cases where courts denied motions to dismiss unjust enrichment claims analogous to his. *Rudolph v. Hudson's Bay Co.*, No. 18-cv-8472 (PKC), 2019 WL 2023713 (S.D.N.Y. May 7, 2019); *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 533–37 (M.D. Pa. 2021); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 412–13 (E.D. Va. 2020). Unlike *Carlsen*, none of these cases is from the Eighth Circuit Court of Appeals, and none purports to apply Minnesota law. Their reasoning is inconsistent with *Carlsen* and *In re Target*, and the Court finds Mr. Hall's reliance on them unavailing.

a result of the data breach, he has experienced "anxiety, sleep disruption, stress, fear, and frustration." [*Id.* ¶ 41.] And he alleges that Centerspace's untimely notification of the data breach prevented him from taking appropriate steps more promptly to protect his PII and mitigate the harm caused by the breach. [*Id.* ¶ 51.]

Other courts have found cognizable damages based on similar allegations at the motion-to-dismiss stage. *Netgain*, 2022 WL 1810606, at *14 ("Courts have held that damages like monitoring and lost time are cognizable.") (collecting cases); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1171 (finding allegations of harm flowing from untimely disclosure of breach sufficient); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021) (discussing the "growing trend across courts . . . to recognize the lost property value of personal information") (ellipses in original, quotations omitted). Although Centerspace has pointed to cases in its briefing that have granted Rule 12(b)(6) motions based on insufficient damages claims, none are binding authority. Moreover, Centerspace has not persuaded the Court that their reasoning is consistent with the most recent trends in this rapidly developing area of the law, nor that the forms of damages sought by Mr. Hall are foreclosed as a matter of substantive Minnesota law. Accordingly, the motion is denied with respect to Centerspace's request to dismiss the negligence or implied-contract claim for failure to plead damages.

ORDER

For the reasons discussed above, the Defendants' Motion to Dismiss [Doc. 13] is **GRANTED IN PART** and **DENIED IN PART** as follows:

1. Plaintiff's claims against Defendant Centerspace, Inc., are hereby **DISMISSED WITHOUT PREJUDICE** based on Plaintiff's agreement;
2. Plaintiff's claims for forward-looking declaratory and injunctive relief are **DISMISSED WITHOUT PREJUDICE** for lack of subject matter jurisdiction;
3. Plaintiff's claim for unjust enrichment in Count III of the Complaint is **DISMISSED** for failure to state a claim; and
4. Defendants' Motion is **DENIED** in all other respects.

Date: May 12, 2023

s/Katherine Menendez
Katherine Menendez
United States District Judge